REMARKS

Claims 1, 3, 5, 7, 8, 10, 12, 14, 16 and 17 are pending in the application. Claims 1, 3, 5, 8, and 10 have been amended. Favorable reconsideration of the application, as amended, is respectfully requested.

I REJECTION OF CLAIMS UNDER 35 USC 35 USC § 101

Claims 1, 3, 5, and 8, stand rejected under 35 USC 101. The applicant has rephrased claim 1 such that the functional descriptive material is embodied on computer readable medium. It also must be noted that the various messages defined in the applicant's claim 1 are not "nonfunctional descriptive material" but are specific limitations further defining the functionally descriptive material and distinguishing the functionally descriptive material over the prior art. Claims 3, 5, and 8 depend from claim 1 making the amendment to claim 1 effective on dependent claims 3, 5, and 8.

II REJECTION OF CLAIMS UNDER 35 USC 35 USC § 103

Claims 1, 3, 5, 7, 8, 10, 12, 14, 16 and 17 stand rejected under 35 USC 103(a) as being unpatentable over US Patent Number 7,111,053 to Black and US Patent 6,519,635 to Champlin and US Patent 5,991,806 to McHann in view of US Patent 7,225,249 to Barry.

General Discussion of Applicant's invention

The Simple Network Management Protocol (SNMP) is a well known communication protocol that enables an SNMP Manager (also known as an SNMP Managing System) to collect data from SNMP managed clients (also known as SNMP managed systems or agents).

It is well known that SNMP utilizes UDP/IP messaging to predefined ports and, as such, an SNMP request can not be sent from an SNMP Manager on the Internet "inbound" to an SNMP managed client that is on a local area network

served by a NAT firewall (e.g. a network utilizing the subset of IP addresses reserved for local area networks).

In a NAT firewall environment message exchanges can only be initiated by the client device on the local network and responded to by the device on the Internet.

With reference to the applicant's Figure 1, the applicant's invention is to a novel sub manager system 20. The sub manager 20 operates, with respect to an SNMP Managing System 22, as an SNMP managed client exchanging SNMP messages in the ordinary course. The sub manager operates, with respect to each SNMP managed client 18, as an SNMP manager – but with the exception that messaging is sent utilizing a connection maintained through the firewall.

A novel sub manager and method for generating SNMP messes to a managed client in response to receipt of a request message is disclosed. In more detail, the SNMP manager 22 sends a master SNMP network management request message to the Sub Manager. The Sub Manager generates and sends SNMP network management requests to each of the clients, each through the connection maintained with such client through the firewall.

A response is received from each client. The responses are aggregated into a single response message back to the SNMP Manager 22.

Claim 1

With reference to Figure 1, the applicant's invention, as specifically defined in claim 1, is to a sub manager 20 for interfacing between an SNMP network management system 22 and a plurality of SNMP managed clients 18. Each of such SNMP managed clients 18a, 18b, 18c is served by a network address translation firewall 16a, 16b.

The sub-manager 20 comprises a network management agent 25. The network management agent: i) receives a master SNMP network management request message 170 (Figure 6 and Figure 8) from the SNMP network management system 22; and ii) provides a master SNMP response message 192

(Figure 6 and Figure 8) to the SNMP network management system (See Page 14, Lines 6-15).

First point of distinction of Claim 1 over Black and other referenced art.

The examiner cites Black C9, L28-58; C27, L42 to C28, L25; and C11, L65 to C12, L12 as disclosing a network management agent for receiving a master SNMP network management request message from the SNMP management system. The examiner further indicates that the applicant's master SNMP network management request is disclosed by Black at C21, L54 to C22, L10; Figure 2a; and C9, 28 to C12, L12.

The applicant respectfully disagrees and asserts that Black does not teach or suggest the applicant's network management agent for receiving a master SNMP network management request message from the SNMP management system.

More specifically, it must be appreciated that the applicant's Claim 1 specifically states that what is received from the SNMP management system is a "master SNMP network management request" Claim 1 further specifically defines what a master SNMP network management request is. More specifically, with reference to Figure 6, the master SNMP network management request message 170 specifically includes a plurality of variable values 176. Each variable value 176 is identified by a master object identifier 182 selected from within a master information base 32. (Figure 6, Page 18, Lines 2-9). With reference to Figure 1, each master object identifier 182 specifically comprises:

i) a client identifier 46 that identifies a particular one of the plurality of SNMP managed clients 18 which has a client management information base 34 that includes the variable value (reference number 44 in the client management information base 34); and

ii) a variable identification portion 210, the variable identification portion 210 being a client object identifier 188 that identifies the variable value 44 within the client management information base 34. (Page 20, Lines 5-11)

It must be noted that all of these limitations exist in the applicant's claim 1. The examiner has not specified how certain generalized teachings of Black (or the other art of record) disclose, or render obvious, the specific claim limitations of the applicant's invention and the applicant respectfully asserts that Black does not teach or suggest the elements the examiner asserts.

Black C9, L28-58 (pasted below for convenience) may teach network management and objectives of network management, but does not does not teach of suggest a network management agent receiving a master SNMP network management request message - as specifically defined by all of the limitations of the applicant's Claim 1 - from an SNMP management system.

Black C9, L28-58 Alternatively, the control and data may be passed over one common path (in-band).

Network/Element Management System (NMS):
Exponential network growth combined with continuously changing network requirements dictates a need for well thought out network management solutions that can grow and adapt quickly. The present invention provides a massively scalable, highly reliable comprehensive network management system, intended to scale up (and down) to meet varied customer needs.

Within a telecommunications network, element management systems (EMSs) are designed to configure and manage a particular type of network device (e.g., switch, router, hybrid switch-router), and network management systems (NMSs) are used to configure and manage multiple heterogeneous and/or homogeneous network devices. Hereinafter, the term "NMS" will be used for both element and network management systems. To configure a network device, the network administrator uses the NMS to provision services. For example, the administrator may connect a cable to a port of a network device and then use the NMS to enable the port. If the network device supports multiple protocols and services, then the administrator uses the NMS to provision these as well. To manage a network device, the NMS interprets data gathered by programs running on each network device relevant to network configuration, security, accounting, statistics, and fault logging and presents the interpretation of this data to the network administrator. The network administrator may use this data to, for example, determine when to add new hardware and/or services to the network device, to determine when new network devices should be added to the network, and to determine the cause of errors.

Black C27, L42 to C28, L25 (pasted below for convenience) may teach a

computer system pushing a JAVA class file (used to interpret a binary file) to the network management server and may also teach the network management system reading a card table and port table to determine what hardware is available in computer system and may teach the NMS assigning a logical identification number to each card and port and inserts these numbers in an LID to PID card table in the configuration database. However, Black C27, L42 to C28, L25 does not teach of suggest a network management agent receiving a master SNMP network management request message - as specifically defined by all of the limitations of the applicant's Claim 1 - from an SNMP management system.

> *Black C27, L42 to C28, L25: Referring to FIG. 9, as described above, a user/network administrator of computer system 10 works with network management system (NMS) software 60 to configure computer system 10. In the embodiment described below, NMS 60 runs on a personal computer or workstation 62 and communicates with central processor 12 over Ethernet network 41 (out-of-band). Instead, the NMS may communicate with central processor 12 over data path 34 (FIG. 1, in-band). Alternatively (or in addition as a back-up communication port), a user may communicate with computer system 10 through a console interface/terminal (840, FIG. 2a) connected to a serial line 66 connecting to the data or control path using a command line interface (CLI) protocol. Instead, NMS 60 could run directly on computer system 10 provided computer system 10 has an input mechanism for the user.*
>
> *During installation, an NMS database 61 is established on, for example, workstation 62 using a DDL executable file corresponding to the NMS database. The DDL file may be downloaded from persistent storage 21 in computer system 10 or supplied separately with other NMS programs as part of an NMS installation kit. The NMS database mirrors the configuration database through an active query feature (described below). In one embodiment, the NMS database is an Oracle database from Oracle Corporation in Boston, Mass.*
>
> *The NMS and central processor 12 pass control and data over Ethernet 41 using, for example, the Java Database Connectivity (JDBC) protocol. Use of the JDBC protocol allows the NMS to communicate with the configuration database in the same manner that it communicates with its own internal storage mechanisms, including the NMS database. Changes made to the configuration database are passed to the NMS database to ensure that both databases store the same data. This synchronization process is much more efficient, less error-prone and timely than older methods that require the NMS to periodically poll the network device to determine whether configuration changes have been made. In these systems, NMS polling is unnecessary and wasteful if the configuration has not been changed. Additionally, if a configuration change is made through some other*

means, for example, a command line interface, and not through the NMS, the NMS will not be updated until the next poll, and if the network device crashes prior to the NMS poll, then the configuration change will be lost. In computer system 10, however, command line interface changes made to configuration database 42 are passed immediately to the NMS database through the active query feature ensuring that the NMS, through both the configuration database and NMS database, is immediately aware of any configuration changes.

Black C11, L65 to C12, L12 (pasted below for convenience) may teach a traditional network management system and further indicate that the NMS database may be remote or local with respect to the networks devices it is managing. However, Black C11, L65 to C12, L12 does not teach of suggest a network management agent receiving a master SNMP network management request message - as specifically defined by all of the limitations of the applicant's Claim 1 - from an SNMP management system.

Black C11, L65 to C12, L12: Selected data stored within NMS database 61 may also be replicated to one or more remote/central NMS databases 854a 854n, as described below. NMS servers may also access network device statistics and status information stored within the network device using SNMP (multiple versions) traps and standard Management Information Bases (MIBs and MIB-2). The NMS server augments SNMP traps by providing them over the conventional User Datagram Protocol (UDP) as well as over Transmission Control Protocol (TCP), which provides reliable traps. Each event is generated with a sequence number and logged by the data collector server in a system log database for in place context with system log data. These measures significantly improve the likelihood of responding to all events in a timely manner reducing the chance of service disruption.

Black C21, L54 to C22, L10, (pasted below for convenience) may teach use of profiles by the NMS to provide individual users with customized graphical user interfaces for viewing of their network with defined management capability. However, Black C21, L54 to C22, L10 does not teach of suggest a network management agent receiving a master SNMP network management request message - as specifically defined by all of the limitations of the applicant's Claim 1 - from an SNMP management system.

> *C21, L54 to C22, L10: Profiles may be used by the NMS client to provide individual users (e.g., network managers and customers) with customized graphical user interfaces (GUIs) or views of their network and with defined management capabilities. For example, some network managers are only responsible for a certain set of devices in the network. Displaying all network devices makes their management tasks more difficult and may inadvertently provide them with management capabilities over network devices for which they are not responsible or authorized to perform. With respect to customers, profiles limit access to only those network devices in a particular customer's network. This is crucial to protecting the proprietary nature of each customer's network. Profiles also allow each network manager and customer to customize the GUI into a presentation format that is most efficient or easy for them to use. For example, even two users with access to the same network devices and having the same management capabilities may have different GUI customizations through their profiles. In addition, profiles may be used to provide other important information, for example, SNMP community strings to allow an NMS server to communicate with a network device over SNMP, SNMP retry and timeout values, and which NMS servers to use, for example, primary and secondary servers may be identified.*

Not only does Black fail to teach of suggest the applicant's invention for these reasons, as discussed in the response to the previous office action, neither Champlin nor the other art of record teaches or suggests the applicants invention as defined by Claim 1.

Second point of distinction of Claim 1 over Black and other referenced art.

As additional claim elements, the applicant's sub-manager 20 of claim 1 further comprises a connections module 24. The connections module 24, for each of the plurality of SNMP managed clients 18a, 18b, 18c, establishes an internet protocol connection 45 with such SNMP managed client 18 through the firewall 16 serving such SNMP managed client 18. (See Page 15, Lines 15-16 and Page 4, Line 30 to Page 5, Line 2).

Through the internet protocol connection 45, the connections module 24 both: i) provides, to each of the plurality of SNMP managed clients 18, a client network management request message 172 (Figure 6, Figure 4b, step 125, Page 17, Lines 14-15); and ii) receiving, from each of the plurality of SNMP managed

clients 18, a client response message 206 (Figure 7, Figure 4b, Step 127, Page 16, Lines 13-14, Page 16, Lines 25-26).

As specifically defined in Claim 1, the client network management request message includes the client object identifier that identifies the variable value within the client management information base (both are specific elements of the Master SNMP network management request message – discussed above).

As specifically defined in Claim 1, the client response message includes the client object identifier and the variable value from the client management information base.

These specific definitions for these specific message are explicit limitations of claim 1 that are not taught or suggested by Black nor other art of record. are limitations included in claim 1 – further defining the applicant's connection module.

With respect to these elements, the examiner references Black C21, L26-42; C11, L65 to C12; and C27, L42 to C28 (all of which are pasted in above for convenience).

The applicant acknowledges that the term TCP/IP connection is used at Black C12, L6-7 and there is a suggestion of reliable traps, however none of the cited passages teach or suggest, for each of the plurality of SNMP managed clients, establishing an internet protocol connection with such SNMP managed client through the firewall serving such SNMP managed client – and through the internet protocol connection, the connections module both: i) provides, to each of the plurality of SNMP managed clients 18, a "client network management request message" as specifically defined in Claim 1; ii) receiving, from each of the plurality of SNMP managed clients 18, a "client response message" as specifically defined in Claim 1.

Further, the examiner acknowledges that Black does not teach the identifying each client in the management information base. The examiner cites Champlin Abstract and C2, L58 to C3, L4 and C4, Lines 49-64 as teaching a client identifier that identifies a particular one of the plurality of SNMP managed clients

that has a client management information base that includes a requested variable value.

These passages of Champlin teach an element Champlin refers to as a PDU. The PDU includes the address of the object to be controlled, a desired command (e.g. Set or Get), and an appropriate value.

Even if it taken that the "appropriate value" of the Champlin PDU is comparable to each variable value 176 of the applicant's master SNMP management request message 170 and, even if it is taken that Champlin's header or address is comparable to applicant's client identifier 46 of the master object identifier 182, Champlin still fails to teach a client object identifier 188 as a portion of the master object identifier 183 (in addition to the client ID) that identifies the variable value within the client management information base 34 – all limitations specifically defining the applicant's connection module.

Therefore, neither Black, Champlin nor the other art of record teaches or suggests this element.

Third point of distinction of Claim 1 over Black and other referenced art.

As yet additional elements, the sub-manager defined in Claim 1 further comprises a message handling module 26. With reference to Figure 6 and Figure 9a and page 15, lines 5-19, the message handling module 26 performs at least the three following steps:

1. Receives the master SNMP network management request message (specifically defined in Claim 1);

2. For each master object identifier included in the master SNMP network management request message, generates the client network management request message (specifically defined in Claim 1); and

3. Generates the master SNMP response message (specifically defined in Claim 1) from each received client response message; and

With respect to these elements, it appears, but is not clear, that the examiner cites Champlin Abstract and C2, Line 58 – C3, L14 and C4, L49-64 as: i) teaching generating the client network management request message for each master object identifier included in the master SNMP network management message; and ii) teaching a client network management request message including a client object identifier that identifies the variable value within the client management information base.

The applicant's invention specifically cites that the client management request message 172 includes the client object identifier 188 that identifies the variable value 44 within the client management information base 34 – noting that the antecedent basis for the client object identifier is within the variable identification portion of the master object identifier of the master network management request message.

In one aspect, Champlin teaches "reformatting an SNP PDU to a format which can be recognized by an associates SNMP sub-agent" (C3, L9-11). In another aspect, Champlin teaches a translation table 70 which apparently provide direct translation between MIB object identifies and database record protocols.

In neither aspect does Champlin teach the applicant's novel system and method for generating client network management request messages from a master network management request message that comprises: i) inclusion of the client object identifier within the variable identification portion of the master object identifier of the master network management request message; and ii) use of such client object identifier for the client network management request message.

For at least these reasons, the applicant respectfully asserts that Claim 1 is allowable over Black Champlin, Barry, McHann, and the other art of record.

Claim 7

Claim 7, which depends from claim 1 and has not been substantively amended, further specifies that the master SNMP network management request message comprises at least two master object identifiers, each master object

identifier comprising a client identifier that is unique from the client identifier of at least one other master object identifier.

The examiner cites McHann C2, L16 to C3, L14; and C4, L49-64 as teaching the master SNMP network management request message comprises at least two master object identifiers, each master object identifier comprising a client identifier that is unique from the client identifier of at least one other master object identifier.

It must be appreciated that Claim 7 depends from claim 1. As such, claim 7 further defines the master SNMP network management request message – previously defined in Claim 1. As discussed, with respect to Claim 1, each master object identifier 182 comprises:

i) a client identifier 46 that identifies a particular one of the plurality of SNMP managed clients 18 which has a client management information base 34 that includes the variable value (reference number 44 in the client management information base 34); and

ii) a variable identification portion 210, the variable identification portion 210 being a client object identifier 188 that identifies the variable value 44 within the client management information base 34. (Page 20, Lines 5-11)

McHann The teachings of McHann fail to teach the master SNMP network management request message (defined in claim 1) further comprising at least two master object identifiers (specifically defined in claim 1), each master object identifier comprising a client identifier that is unique from the client identifier of at least one other master object identifier (all as specifically defined in claim 1).

For at least these reasons, in addition to the reasons described with respect to independent claim 1, the applicant respectfully asserts that Claim 7 is allowable over Black, Champlin, Barry, McHann, and the other art of record.

Claim 3

Claim 3, as amended and depending from claim 7, further specifies that each internet protocol connection 45 is a TCP/IP connection that is established

with the SNMP managed client 18, through the firewall 16 serving such SNMP managed client in response to receiving a connection request initiating by such SNMP managed client (Figure 4a, step 116 and Page 15, 17-19).

The connections module 24 further records, in response to receiving an SNMP inform message from the SNMP managed client 18 through the internet protocol connection 45, the SNMP inform message including the SNMP managed client's client identifier 46:

1) spawns a device state machine for the SNMP managed client (Page 15, Lines 23-28); and

2) records in an active connections table 28 and in association with the client identifier 46:

i) a client connection identifier 48, the client connection identifier comprising the source IP address 50 and source port number 52 of the SNMP inform message initiated by the SNMP managed client and translated by the firewall serving the client; and

ii) a device state machine identifier identifying the device state machine (Figure 1, Figure 4a, and Page 15, Line 29 to Page 16, Line 7); and

the device state machine provides the client network management request message to the SNMP managed client by providing the client network management request message over the internet protocol connection that associates, in the active connections table, with the client identifier of the master object identifier.

With respect to these elements, the examiner cites Black C11, L65 to C12, L12 (pasted in above) and C27,L42 to C28, L25 (pasted in above). Such passages may discuss TCP/IP connections and indicated that a reliable trap is suggestible, but the applicant's invention is not just a concept of a reliable trap – it is a unique system embodying many elements. The passages fail to disclose the combination of claim limitation defining the applicant's claim 3 (as it includes the limitations of Independent Claim 1 and intervening claim 7).

For at least these reasons, in addition to the reasons described with respect to independent claim 1 and intervening claim 7, the applicant respectfully asserts that Claim 3 is allowable over Black, Champlin, Barry, McHann, and the other art of record.

Claim 5

Claim 5, which has been amended to depend from claim 7 but not otherwise substantively amended, further defines the device state machine as providing for:

periodically receiving a heart beat message from the SNMP managed client over the internet protocol connection; each heart beat message including the client identifier and a time interval between the heart beat message and a subsequent heart beat message;

updating the client connection identifier in the active connection table if the source IP address or the source port number obtained from the heart beat message differs from that of a previous heart beat message;

providing a heart beat acknowledgement message to the SNMP managed client over the internet protocol connection; and

determining that the internet protocol connection is inactive if a time period in excess of the time interval elapses during which a subsequent heart beat message has not been received.

With respect to these elements, the examiner generally cites McHann Abstract, C10, Line 34 to C11, Line 60 as teaching: i) receipt of a heart beat message including the client identifier; ii) updating the client connection identifier in the active connections table if the source IP address or the source port number obtained form the heart beat message differs from a previous heart beat messaging and providing a heart beat acknowledgement to the SNMP managed client.

The applicant respectfully disagrees. McHann Figures 4 and 5 depict a well known SNMP architecture wherein a Managing System 402 (Figure 4, 502 in Figure 5) utilizes SNMP management protocols to communicate with one or more

Agents 412 of the Managed Systems (404 in Figure 4, 504 in Figure 5). As is well known in the art of network management, the SNMP management protocols utilize UDP/IP messaging over an IP compliant network.

With reference to Figure 1, McHann teaches a message router 104 which executes on a computer system 102 and determines local computer system events such as (ACPI, SMI, PnP, DMI, an OS events) and generates messages in a common format that may be sent over a network 104. SNMP is a representative common format.

In more detail, McHann teaches a software application (Dynamic System Control 810 as depicted in Figure 8) which resides on one of the managed systems. The DSC 810 monitors local events on the system bus (such as DMI, SMI, OS or other system messages) and generates common format messages (e.g. SNMP messages) to the Managing System over the IP network 802 (note, network 802 is near the bottom of McHann Figure 8, it is unknown why the processor is also labeled 802).

The DSC 810 monitors the system bus to detect such "lower level" local events or otherwise receives such local events – and passes common format (e.g. SNMP messages) up to the SNMP Managing System. The system components are not SNMP managed clients and there is no teaching in McHann of requesting information from any of the system components.

With specific respect to McHann's teachings of signaling at C10, Line 34 to C11, Line 60, the applicant asserts that such signaling across a system bus internal to the computer system (202 in Figure 2, unlabeled in Figure 8) which specifically is not SNMP messaging – and there is no internet protocol signaling across the system bus, no IP addressing across the system bus, nor are source port number usage.

McHann utilizes the term "network" interchangeably to refer to both the system bus and the IP network 100 (Figure 1) – with are entirely different structures with entirely different functions. Such unorthodox and interchangeable use of the term "network" does not in any way teach, suggest, nor enable SNMP signaling

(which occurs on the IP network 100 of McHann) on the system bus – nor does such interchangeable use of language teach or suggest that SNMP signaling is interchangeable with the local computer system event signals sent over the system bus 202.

For this reason, the applicant respectfully traverses the examiners position that local computer system events sent over the system bus 202 as described at C10, Line 34 to C11, Line 60 teaches or suggests the applicant's invention as described in Claim 5.

For at least these reasons, in addition to the reasons described with respect to independent claim 1 and intervening claims 7 and 3, the applicant respectfully asserts that Claim 5 is allowable over Black Champlin, Barry, McHann, and the other art of record.

Claim 6

Claim 6 depends from claim 6 and is distinguishable over Black, Champlin, McHann, and Barry for at least the reasons described with respect to independent claim 1 and intervening claims 7, 3, and 5.

Claim 8

Claim 8 depends from claim 7 and is distinguishable over Black Champlin, McHann, and Barry for at least the reasons described with respect to independent claim 1 and intervening claim 7.

Claims 10, 12, and 14-17

Claims 10, 12, and 14-17 are method claims of substantially the same scope as claims 1, 3, and 5-8 respectively. Claims 10, 12, and 14-17 are therefore distinguishable over Black, Champlin, McHann, and Barry for at least the same reasons as discussed with respect to claims 1, 3, and 5-8.

III. CONCLUSION

Serial No.: 10/713,481

Accordingly, Claims 1, 3, 5-8, 10, 12, and 14-17 are believed to be allowable and the application is believed to be in condition for allowance. A prompt action to such end is earnestly solicited.

Should the Examiner feel that a telephone interview would be helpful to facilitate favorable prosecution of the above-identified application, the Examiner is invited to contact the undersigned at the telephone number provided below.

Respectfully submitted,

Timothy P. O'Hagan
Reg. No. 39,319

DATE: 1-20-09

Timothy P. O'Hagan
8710 Kilkenny Ct
Fort Myers, FL 33912
(239) 561-2300